B-GROUPS

by

ALBERT BUCKLEY

A THESIS

SUBMITTED TO THE FACULTY OF GRADUATE STUDIES

IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE

OF MASTER OF SCIENCE

DEPARTMENT OF MATHEMATICS

UNIVERSITY OF ALBERTA

EDMONTON, ALBERTA

APRIL, 1968

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

UNIVERSITY OF ALBERTA

FACULTY OF GRADUATE STUDIES

The undersigned certify that they have read and recommend to the Faculty of Graduate Studies for acceptance, a thesis entitled "*B*-Groups", submitted by ALBERT BUCKLEY in partial fulfilment of the requirements for the degree of Master of Science.

ABSTRACT

This thesis is devoted to a study of Schur's theory as applied to the study of B-groups, and specifically to examination of the structure of specific S-rings over certain Abelian groups.

Chapter I presents the fundamentals of Schur's theory, including a brief introduction to the pertinent permutation group theory. A survey of known results appears in Chapter II, and all non-trivial primitive S-rings over Abelian groups of order up to 50 are presented in Chapter III. Finally, in Chapter IV it is shown that an Abelian group of order 72 is a B-group.

ACKNOWLEDGEMENTS

I would like to thank my supervisor, Dr. R.D. Bercov, for his assistance, guidance and patience during preparation of this thesis; further, I would like to express my gratitude to Dr. F.I. Gross, whose teaching enthusiasm helped to generate the interest necessary to undertake and complete the thesis.

TABLE OF CONTENTS

CHAPTER I

SCHUR THEORY

§1.1 Introduction

In this chapter we will develop, without proofs, the essential parts of Schur's theory (8) which are to be used in the following chapters. In the discussion of permutation group theory only those results will be included which are necessary for the development of Schur's method; many interesting aspects of this theory will thus be only briefly, or not, mentioned.

§1.2 Permutation groups

Letting Ω be any set of n elements, we denote by S^{Ω} the set of one-to-one mappings from Ω onto itself. For $\alpha \in \Omega$ and $g \in S^{\Omega}$ we designate the image of α under the mapping g by α^g. For $g_1, g_2 \in S^{\Omega}$ we define their product by $\alpha^{g_1 g_2} = \left(\alpha^{g_1}\right)^{g_2}$, an operation which clearly makes S^{Ω} a group of order $n!$. S^{Ω} is referred to as the *symmetric group* on n letters; we will call a subgroup G of S^{Ω} (denoted $G \leq S^{\Omega}$) a *permutation group*. We note that the *degree* of G refers to the number of letters of Ω not fixed by G.

We now wish to examine Ω from the point of view of its subsets, for these will provide the basic tools for Schur's theory. For $\Delta \subseteq \Omega$ and $K \subseteq G$ define $\Delta^K = \{\delta^k : \delta \in \Delta \text{ and } k \in K\}$. Then Δ is a *block* of G if $\Delta^g (= \Delta^{\{g\}}) = \Delta$ or $\Delta^g \cap \Delta = \emptyset$ for all $g \in G$. If the latter case never occurs, Δ is a *fixed block*; a minimal fixed block is called an *orbit* of G. Clearly each $\alpha \in \Omega$ lies in exactly one orbit α^G of G, so the orbits of G

provide a disjoint subdivision of Ω. Furthermore, orbits are related to subgroups of G, for defining $G_\alpha = \{g \in G : \alpha^g = \alpha\}$, and noting that $|S|$ denotes the number of elements of the finite set S, we see that

1.2.1 $$|G_\alpha| \cdot |\alpha^G| = |G| .$$

§1.3 Transitive, primitive and regular permutation groups

As these properties will be of primary concern throughout the thesis, a brief discussion of them is in order. We call $G \leq S^\Omega$ *k-transitive* on $\Delta \subseteq \Omega$, $|\Delta| \geq k$, when, for every pair of ordered k-tuples $(\alpha_1,\ldots,\alpha_k)$ and $(\beta_1,\ldots,\beta_k)$ from Δ such that $\alpha_i \neq \alpha_j$ and $\beta_i \neq \beta_j$ for $i \neq j$, we have a $g \in G$ such that $\alpha_i^{\,g} = \beta_i$ for $i = 1,\ldots,k$. We refer to 1-transitive as transitive, 2-transitive as doubly transitive, and easily see that G is transitive on a fixed block Δ if and only if Δ is minimal. We easily obtain the following important result.

Theorem 1.3.1.

Let G be transitive on Ω and choose $\alpha \in \Omega$. Then G is $(k+1)$-transitive on Ω if and only if G_α is k-transitive on $\Omega-\{\alpha\}$.

Using 1.3.1, and noting that $|\alpha^G|$ is the degree of G whenever G is transitive on Ω, we obtain, by repeated application of 1.2.1,

Theorem 1.3.2.

If G is k-transitive on Ω, and of degree n, then

$$n(n-1)\ldots(n-k+1) \mid |G| .$$

A transitive group $G \leq S^\Omega$ is *primitive* on Ω when it has only the trivial blocks $\emptyset, \{\alpha\}$ and Ω. We use the term *uniprimitive* to mean

primitive but not doubly transitive. The following provides an essential criterion for primitivity.

Theorem 1.3.3.

Let $\alpha \in \Omega$ with $|\Omega| > 1$. Then a transitive group G on Ω is primitive if and only if G_α is a maximal subgroup of G.

We will call a permutation group G on Ω *semi-regular* if $G_\alpha = \{1\}$ for all $\alpha \in \Omega$, and *regular* if it is both semi-regular and transitive. Clearly, by virtue of 1.2.1, the order of a semi-regular group divides its degree; thus, by 1.3.2, we obtain

Theorem 1.3.4.

A transitive permutation group is regular if and only if its degree and order are equal.

At this point it is in order to define a *Burnside group* (*B-group*) — although it is not presently necessary — as a group which cannot be imbedded regularly as a subgroup of a uniprimitive group.

§1.4 *S*-modules

With this brief introduction to permutation groups, we will now introduce a restriction which provides the fundamental motivation for Schur's method (8). We wish to regard G not as a permutation group on arbitrary elements, but as acting on elements related by a group structure. This we accomplish as follows. Let H be a regular group on Ω and distinguish a point $\alpha \in \Omega$. Since H is regular, for any $\beta \in \Omega$ there is a unique $h \in H$ such that $\alpha^h = \beta$; with β associate this h. Thus we can consider $G \leq S^\Omega$ as a permutation group on H, for, given $g \in G$ we

define h^g, for $h \in H$, to be that element of H associated with α^{hg}. That is, h^g is that (unique) element of H such that $\alpha^{h^g} = \alpha^{hg}$. No notational difference will distinguish $G \leqslant S^{\Omega}$ and $G \leqslant S^{H}$, for no confusion should result. In the following we assume that $H \leqslant G$, in which case it is obvious that $h,k \in H$ means $h^k = hk$ and that G_1 corresponds to G_α.

Next we introduce the *group ring* $R(H)$ of an abstract group H over a ring R with identity as $\{\sum_{h\in H} c_h h : c_h \in R\}$. Thus $R(H)$ is the set of formal linear combinations of elements of H for which we define addition termwise and multiplication distributively over the elements of H. We see then that $R(H)$ is certainly a ring as well as a left module over R. We take the liberty of saying that $h \in \eta \in R(H)$ when h appears in η with a non-zero coefficient, and that $\eta = \sum_{k\in K} c_k k$ indicates that $\eta \in R(H)$ having the given coefficients for $k \in K \subseteq H$ and zero coefficient for $k \notin K$. We call $|\eta| = \sum_{h\in H} c_h$ the *length* of η.

We now wish to apply these constructions to our study of permutation groups, where throughout this thesis R is the set of rational integers. We call $\eta \in R(H)$ *simple* when $\eta = \sum_{k\in K} k$ for some $K \subseteq H$; given $K \subseteq H$ we denote $\sum_{k\in K} k$ by $\overline{K}$.

As in §1.2, G decomposes H into orbits $T_1,\ldots,T_k$; we now define the *Schur module* (S-module) $R(H,G)$ as the module spanned by $\overline{T}_1,\ldots,\overline{T}_k$, which we call a basis for $R(H,G)$. That is, $R(H,G) = \{\sum_{i=1}^{k} c_i\overline{T}_i : c_i \in R\}$. In order to decide if an arbitrary submodule of $R(H)$ is an S-module for some group G, we state

Theorem 1.4.1.

Choose a submodule S of $R(H)$. Then S is an S-module if and only if S has a basis of simple quantities whose sum is $\overline{H}$.

Proof: The sufficiency follows by considering the group G generated by the cycles whose elements are those of the basis elements. Necessity is clear.

With S an arbitrary S-module, $\eta = \sum_{h\in H} c_h h \in S$, and $\eta^* = \sum_{h\in H} c_h h^{-1}$, we immediately obtain from the existence of a basis the following results.

1.4.2 Choose $c \in R$. Then $\overline{\{h \in \eta : c_h = c\}} \in S$.

1.4.3 $\overline{\{h \in \eta\}} \in S$.

1.4.4 Let $f: R \to R$ be single valued. Then $f[\eta] = \sum_{h\in H} f(c_h) h \in S$.

1.4.5 For $\eta, \zeta \in S$ and $a, b \in R$, $\eta^{**} = \eta$, $(a\eta + b\zeta)^* = a\eta^* + b\zeta^*$, $(\eta\zeta)^* = \zeta^*\eta^*$ and $\eta\eta^* = 0$ only for $\eta = 0$.

We note that these results are mentioned for completeness because they are vital to later proofs, even though their roles in these proofs may not be explicitly mentioned.

§1.5 S-rings

We now introduce the basic tool of Schur's theory, the *Schur-ring* or *S-ring*, whose properties will be linked with properties of corresponding groups, as an S-module over H which is a subring of $R(H)$ containing 1, and containing η^* whenever it contains η. An S-ring S will be termed *primitive* when $K \leq H$ and $\overline{K} \in S$ imply $K = \{1\}$ or H. The special primitive S-ring whose basis is $\overline{\{1\}}$ and $\overline{H^{\#}}$ (where $H^{\#}$ denotes $H-\{1\}$) can be characterized as the intersection of all S-rings over H, and is referred to as the *trivial S-ring*. The following properties are easily

proven (13, p.57), but have important consequences. S is an arbitrary S-ring; $\langle K\rangle$ denotes the subgroup of H generated by $K \subseteq H$.

1.5.1 Choose $\eta \in S$ with $M = \{h \in H : \eta h = \eta\}$. Then $M \leq H$ and $\overline{M} \in S$.

1.5.2 Choose a non-zero $\eta \in S$. Then $\overline{\langle\{h \in \eta\}\rangle} \in S$.

Since a primitive S-ring contains only the (simple quantities corresponding to the) trivial subgroups of H, we easily see from 1.5.1 and 1.5.2 that:

1.5.3 If S is primitive and $S \ni \eta \neq c\cdot\overline{\{1\}}$, then $\langle\{h \in \eta\}\rangle = H$.

1.5.4 If S is primitive and $S \ni \eta \neq c\cdot\overline{H}$, then $\eta h = \eta$ implies $h = 1$.

We now wish to introduce a theorem due to Schur (8) which is fundamental in the application of S-rings to the study of B-groups. As well, one important consequence, due also to Schur, is stated.

Theorem 1.5.5.

Let G be a permutation group containing the regular subgroup H. Then $R(H,G_1)$ is an S-ring.

Theorem 1.5.6.

G is a primitive permutation group if and only if $R(H,G_1)$ is a primitive S-ring over the regular subgroup H; and G is doubly transitive if and only if $R(H,G_1)$ is trivial.

§1.6 Rationality

We now wish to discuss a concept which greatly simplifies the investigation of an S-ring S over an Abelian group H. Adopting the

notation that $\eta^{(m)} = \left(\sum c_h h\right)^{(m)} = \sum c_h h^m$ for integer m and $\eta \in S$, and that $\sum c_h h \equiv \sum d_h h \pmod p$ means $c_h \equiv d_h \pmod p$ for all $h \in H$, we note (13, p.58)

Theorem 1.6.1.

Choose S, an S-ring over the Abelian group H of order n, m, an integer, and $\eta \in S$. Then

(i) if $(m,n) = 1$, $\eta^{(m)} \in S$;

(ii) if $m = p \mid n$ and S is primitive, $\eta^{(p)} \equiv \delta \cdot 1 \pmod p$ for some $\delta \in R$.

Consequently the following definitions are quite reasonable for S-rings over Abelian groups. As introduced by Schur, for $(m,n) = 1$ we call $\eta^{(m)}$ a *conjugate* of $\eta \in S$, and we call the *trace* of η, $tr\,\eta$, the sum of the distinct conjugates of η. Given a basis $\eta_0 = e, \eta_1, \ldots, \eta_k$, we call the set of distinct traces of the η_i the rational closure of the given basis. For $\{a_1, \ldots, a_m\} \subseteq H$, we denote $tr\overline{\{a_i\}}$ by $tr(a_1 + \ldots + a_m)$. A *rational* $\eta \in S$ is one which is its own trace; a rational S-ring, one consisting only of rational quantities. In the search for S-rings rationality becomes a useful concept, for consider (8)

Theorem 1.6.2.

Let S be a non-trivial S-ring over an Abelian group H with a basis $\eta_0 = e, \eta_1, \ldots, \eta_k$ whose rational closure is $\zeta_0 = e, \zeta_1, \ldots, \zeta_r$. Then the submodule of $R(H)$ spanned by $\zeta_0, \ldots, \zeta_r$ is a rational S-ring over H.

Another simple result with important consequences is

Theorem 1.6.3.

Choose a basis element η of an S-ring S. If there are $x, y \in tr\,\eta$ such that $x^p = y^q = 1$ for different primes p and q, then η is rational.

Clearly these two theorems greatly restrict the irrational S-rings over an Abelian group S of non-prime order for which the rational S-rings are known. Further, if an irrational S-ring has basis elements $\eta_0 = e, \eta_1, \ldots, \eta_k$, then because $|\eta_i| = |\eta_i^{(m)}|$ for $(m,|H|) = 1$, we will have that the distinct traces of the η_i form a rational S-ring whose basis elements have lengths which are multiples of the lengths of the irrational basis elements. These ideas are used repeatedly in Chapters III and IV to find S-rings.

§1.7 Groups of small order

Scott (10, p.408) has developed several results which apply to any finite group, but which are useful only for groups of "reasonably small" order. We assume throughout this section that S is a non-trivial primitive S-ring over a group H of non-prime order, η is an arbitrary basis element, and ζ is the basis element of maximal length. Scott shows $|\eta| \geqslant 3$ and states a very useful result,

Theorem 1.7.1.

If η_1, η_2 and η_3 are basis elements of S for which $\eta_1\eta_2 = i\eta_3 + \ldots$, $\eta_2\eta_3^* = j\eta_1^* + \ldots$, and $\eta_3^*\eta_1 = k\eta_2^* + \ldots$, with $i,j,k \in R$, then $i|\eta_3| = j|\eta_1| = k|\eta_2|$.

Knowing i, j or k then, we can determine the remaining two. Strengthening our hypothesis, we have

Theorem 1.7.2.

If ξ is an arbitrary basis element such that $(|\eta|,|\xi|) = 1$, then $\eta\xi = i\nu$ where $i \in R$ and ν is a basis element such that $|\nu| > \max\{|\eta|,|\xi|\}$.

Several important corollaries result.

Corollary 1.7.3.

$(|\eta|,|\zeta|) > 1$.

Corollary 1.7.4.

If $|H| = p+1$ with $p > 2$, then $|\zeta|$ is not a prime power. Further, there are basis elements of at least 3 different lengths.

Corollary 1.7.5.

If S has a basis $\eta_0 = e, \eta_1, \ldots, \eta_k$ with $|\eta_1| \leq \ldots \leq |\eta_k|$, then $|\eta_1| \cdot |\eta_i| \geq |\eta_{i+1}|$ for $i = 1, \ldots, k-1$.

From these theorems Scott (10, p.408) has shown that there are no non-trivial primitive S-rings over any group of order $p+1$ for $2 < p \leq 37$.

We now introduce the notation, to be used throughout the thesis, that S has orbit pattern $a_1 - \ldots - a_k$ when S has a basis $\eta_0 = e, \eta_1, \ldots, \eta_k$ in which $|\eta_i| = a_i$ for $i = 1, \ldots, k$. It will be generally assumed that the basis will be given in order of ascending length.

Thus, given H, we do not need to consider an arbitrary disjoint subdivision of H as a possible basis for a non-trivial primitive S-ring over H, for the theorems of this section permit only particular orbit patterns. However, application of the theorems beyond $|H| = 32$ becomes a lengthy procedure, although a computer makes the procedure useful somewhat further.

CHAPTER II

B-GROUPS

§2.1 Introduction

In this chapter we will answer, for certain classes of groups, the question of whether an abstract group can be imbedded as a regular subgroup of a uniprimitive group. For many Abelian groups the answer is known, but there are some notable exceptions, one of which will be discussed in Chapter IV.

By Cayley's Theorem (10, p. 48) we know that any group can be represented isomorphically as a regular permutation group, called its right regular representation, on its own elements. Thus for a given abstract group H we assume the group G contains the right regular representation of H. Then, as defined in §1.2, H is a *B-group* when G cannot be uniprimitive. An easy consequence of 1.5.6, which provides the link between Schur's theory and B-groups, is

Theorem 2.1.1.

H is a B-group if the only primitive S-ring over H is the trivial one.

The terminology honors Burnside (2) who in 1911 found the first such group, namely, a cyclic group of non-prime prime power order.

§2.2 The Wielandt Counterexample

Having noted the existence of B-groups, we now exhibit a class of groups which can be imbedded regularly in uniprimitive groups.

Wielandt (13, p.67) constructs a transitive, uniprimitive group G containing as a subgroup any member H of the class of groups given below in Theorem 2.2.1, but he does not give the basis for the generated S-ring $R(H,G_1)$. In order that we recognize this Wielandt S-ring in Chapter III, we will give the basis and show directly that it generates an S-ring, although the basis can in fact be easily obtained from Wielandt's work.

Theorem 2.2.1.

A group H of the form $H_1 \times \ldots \times H_d$ with $|H_1| = \ldots = |H_d| > 2$ and $d > 1$ is never a B-group.

To demonstrate a basis, we define $h \in H_1 \times \ldots \times H_d$ to have length $l(h) = r$ if exactly r elements h_i in the (unique) expansion $h = h_1 \ldots h_d$, where $h_i \in H_i$, are not unity. And now we have

Theorem 2.2.2.

Choose H as in Theorem 2.2.1. Then there is a non-trivial primitive S-ring over H whose i^{th} basis element η_i consists of the elements of H of length i, for $i = 0,\ldots,d$.

Proof: The only property not clear for the submodule spanned by the η_i is the ring property. However, this follows simply, for by symmetry all elements of $\eta_i\eta_j$ of equal length appear with equal coefficient.

§2.3 Known B-groups

As was mentioned in §2.1, Burnside has provided us with one class of B-groups. His approach used group characters, but Schur's method was required to provide in 1933 (8) the first extension of this result

by dropping the prime power condition. Using Schur's method, Wielandt (11) in 1935 generalized this to

Theorem 2.3.1.

Any Abelian group of composite order with a cyclic Sylow subgroup is a B-group.

Although not unreasonable, the extension to all Abelian groups of non-prime order, as conjectured in 1921 by Burnside, is invalid as was seen in §2.2. The results have been extended, however, for by using group characters, D. Manning (5) removed the cyclic limitation by showing, in 1936,

Theorem 2.3.2.

Any Abelian group which can be written as $H_1 \times H_2$ with $|H_1| = p^\alpha$, $|H_2| = p^\beta$ and $\alpha > \beta$ is a B-group unless $\alpha = 1$.

Manning's proof contains an error, but fortunately Kochendörffer (4) has produced an independent proof in 1937 using Schur's method.

With $\exp B$ defined as the smallest positive integer m such that $x^m = 1$ for all $x \in B$, $\langle a \rangle$ defined as the subgroup generated by a, and $o(a) = |\langle a \rangle|$, we have the most general result to date, due to Bercov (3), also using Schur's method, in 1965.

Theorem 2.3.3.

Let the Abelian group H have a Sylow p-subgroup which can be written as $\langle a \rangle \times B$ where $o(a) = p^\alpha$ and $\exp B = p^\beta < p^\alpha$. If $B \neq \{1\}$ (and if $\alpha > 2$ when $p = 2$) and H cannot be written as a direct product of two or more subgroups of the same order greater than 2, then H is a B-group.

The theorem is stated for $B \neq \{1\}$ because the case $B = \{1\}$ is covered by Theorem 2.3.1; if H is a direct product of the kind described, Theorem 2.2.1 applies. However, there do remain some Abelian groups for which it is not known whether they are B-groups or not. Apart from groups which are the direct product of two subgroups of the same exponent, the only groups not covered by Bercov's and Wielandt's results are those of the form $\langle a \rangle \times B \times C$ where $a^4 = 1$, $\exp B = 2$ and C is the direct product of groups of equal exponent. The smallest such H for which it was not previously known as a B-group or not is of order 72. In Chapter IV we show that it is indeed a B-group.

Groups of order 2^m are covered by Theorem 2.2.1 unless m is a prime p. In this case Wielandt (13, p.69) mentions that only when 2^p-1 is also prime may the group be a B-group.

The non-Abelian case has been investigated less thoroughly. As discussed in §1.7, Scott has demonstrated that groups of order $p+1$ with $2 < p \leq 37$ are B-groups. Wielandt (12) has considered the simplest non-commutative case:

Theorem 2.3.4.

Every dihedral group is a B-group.

We also mention:

Theorem 2.3.5, Scott (9).

Every generalized dicyclic group (defined by $x^{2n} = 1$, $y^2 = x^n$, $y^{-1}xy = x^{-1}$) is a B-group.

Theorem 2.3.6, Nagai (6) and Nagao (7).

Let the prime p be of the form $2\cdot 3^{a}+1$ or $6l+1$ where $a > 2$ and $l > 7$. A non-Abelian group of order $3p$ is a B-group.

[illegible]

[illegible]

[illegible]

[illegible]

CHAPTER III

SPECIFIC S-RINGS

§3.1 Introduction

In this chapter we will investigate the S-rings admitted by those Abelian groups whose order does not exceed 50. This will include those groups discussed in §2.2 in order to show that other *NTP*(non-trivial primitive) S-rings besides the Wielandt S-ring can occur, and thus indicate, perhaps, likely prospects for *NTP* S-rings over other groups. In addition, even though no *NTP* S-rings exist (§1.7), the case $|H| = 32$ will be considered in detail, for Scott did not give a proof of this result.

Section 3.2 will introduce the notation and ideas to be used in the remainder of the thesis, and the remainder will be devoted to specific cases. It should be noted that in many cases a computer was used to obtain partial results, and that in some cases from the programming experience it was seen how to complete most of the analysis without use of the machine. In most cases Scott's procedure (§1.7) was applied to ascertain the allowable orbit patterns; only those permitted by Scott are discussed.

At this point it is important to define the concept of equivalent S-rings. We say that two S-rings which can be formed in the same way from isomorphic images of a given group are *equivalent*, and we do not consider them different. The presence of "WLOG" to indicate "without loss of generality" will generally indicate a use of the equivalence relation.

§3.2 Notation

We will let $\eta_0 = e, \eta_1, \ldots, \eta_k$, where $|\eta_1| \leq \ldots \leq |\eta_k|$, be a basis for an arbitrary rational *NTP* *S*-ring over an Abelian group H of order n; η will designate an arbitrary η_i. In the irrational case we will consider $\eta_0, \ldots, \eta_k$ to be a rational closure for some unknown irrational basis which we will denote by $\eta_i = \sum_{j=1}^{t_i} \theta_{ij}$; in general we will write $\eta = \sum_{i=1}^{t} \theta_i$, with θ denoting an arbitrary θ_i. We also note that θ_i, $i = 2, \ldots, t$ are the distinct conjugates of θ_1. As mentioned in §3.1, Scott's procedure (§1.7) is first applied to a given H to determine the allowable orbit patterns. Consequently, when analysis rests on the length of η_1, no mention will be made of values of $|\eta_1|$ not occurring in admissible patterns.

The basis theorem for finite Abelian groups (10, p.92) will be used to write each H as a direct product of cyclic subgroups of prime power order. We adopt the notation that $K_d = \{h \in H : o(h) = d\}$ and that $K_{d_1,d_2} = K_{d_1} \cup K_{d_2}$. As well, we write N for $\{h \in \eta\}$, and define $\eta(h)$ for $h \in H$ to be the coefficient of h in η^2; $\eta(M)$ indicates the common coefficient of all $h \in M$. When $n = 36$ or 72, we have $n = 2^\beta \cdot 3^2$, so by 1.6.1, $\eta^{(2)} \equiv \gamma_2 \cdot 1 \pmod 2$ and $\eta^{(3)} \equiv \gamma_3 \cdot 1 \pmod 3$ for some integers γ_2, γ_3. These conditions will be referred to as δ_2 and δ_3, respectively.

Our general approach to the problem of finding *NTP* *S*-rings will be to pick a length for η, to choose $|\eta|$ distinct elements from H to form η, and to determine if these elements satisfy the ring condition $\eta^2 = \sum_{i=0}^{k} c_i \eta_i$, for some integers c_i, in the respect that all elements of η must occur with equal coefficient in η^2. The choice of these elements

is not arbitrary, for they must satisfy several conditions. In the rational case, each element must appear with all its conjugates, and since all elements associated as conjugates have the same trace, we must in fact choose traces to form η. We will however indicate the trace by one of its elements. Because only the elements of $K_{3,6}$ have a square of order 3 when $n = 36$ or 72, δ_2 requires that the elements of $N \cap K_{3,6}$ occur in pairs of traces with equal 3-part. We will write $r = |\eta|$ and $s = |N \cap K_2|$ so that, since only elements of order 2 are their own traces, r is even if and only if s is. It should be noted at this time that if we find an acceptable η whose square can be written $k_1\eta + k_2(\overline{H^{\#}} - \eta)$, it is then true that η and $\overline{H^{\#}} - \eta$ form a basis for a *NTP* *S*-ring.

A reasonably detailed explanation of basic procedures followed will be given where necessary, but consequent similar explanations will certainly be briefer. Section 3.6 contains the most detailed discussion, for the ideas used there are repeated to obtain the new result given in Chapter IV.

§3.3 The case $n = p$

Within this section we will only consider irrational bases, for clearly a rational basis is trivial. Since the cases with $p < 7$ may be trivially excluded, we assume $p \geq 7$, and we choose any divisor d ($\neq p-1$) of $p-1$. Because the non-zero integers (mod p) form a cyclic multiplicative group R_p, there exists a (unique) subgroup $R_d < R_p$ of order d. (10, p. 35). Choose $\eta = \sum_{k \in R_d} a^k$, where $H = \langle a \rangle$ with $a^p = 1$.

We now wish to show that η and its conjugates form a basis for a *NTP* S-ring. It is, incidentally, easily verified that all basis elements must be of this form. First, a conjugate of η can clearly be written as $\sum_{k\in R_d} a^{kx}$ for some $x\in R_p$; clearly then the distinct cosets of R_d define the distinct conjugates of η. Consequently we need only demonstrate the ring property for the product of two conjugates $\eta^{(s)}$ and $\eta^{(t)}$. To show this, it suffices to show that any two elements a^{k_1y}, a^{k_2y} of $H^{\#}$ have the same coefficient in $w=\eta^{(s)}\cdot\eta^{(t)}$. If they did not, then $w^{(k_1k_2^{-1})}$ would differ from w. However

$$w = \sum_{k\in R_d} a^{ks} \cdot \sum_{k'\in R_d} a^{k't} = \sum_{k,k'} a^{ks+k't} .$$

Thus $$w^{(k_1k_2^{-1})} = \sum_{k,k'} a^{k_1k_2^{-1}ks+k_1k_2^{-1}k't} = w .$$

We conclude that for each divisor d of $p-1$ we generate exactly one *NTP* S-ring; there are, as mentioned, no others.

§3.4 The case $n=p^2$, $p>2$

We will consider an arbitrary p in the rational case but give individual consideration to the cases $n=9$, 25 and 49 for irrational S-rings. In each case we assume $H=\langle a\rangle\times\langle b\rangle$ with $a^p=b^p=1$, and define $\zeta_i=\overline{\langle ab^i\rangle^{\#}}$ for $i=0,\ldots,p-1$, with $\zeta_p=\overline{\langle b\rangle^{\#}}$. Clearly each ζ_i is rational and $\sum_{i=0}^{p}\zeta_i=\overline{H}$. We note first that $\zeta_i\zeta_j=\overline{H^{\#}}-\zeta_i-\zeta_j$ for $i\neq j$, and $\zeta_i^2=(p-1)e+(p-2)\zeta_i$. Clearly $\langle\{h\in\zeta_i\}\cup\{h\in\zeta_j\}\rangle=H$ if and only if $i\neq j$, so that we only need to demonstrate the ring property to conclude that forming each of $\xi_1,\ldots,\xi_r$, $1<r<p$, as a sum of two or more of the

ζ_i such that $\sum_{i=1}^{r} \xi_i = \overline{H^\#}$, together with $\xi_0 = e$, will form a basis for a *NTP* S-ring. However, with $\xi_i = \sum_{k=1}^{u_i} \zeta_{i_k}$ and $\xi_j = \sum_{k=1}^{u_j} \zeta_{j_k}$, we see that

$\xi_i^2 = (p-1)u_i \cdot e + [p-2 + (u_i-2)(u_i-1)]\xi_i + u_i(u_i-1)(\overline{H^\#}-\xi_i)$ and

$\xi_i\xi_j = (u_i-1)u_j\xi_i + u_i(u_j-1)\xi_j + u_iu_j(\overline{H^\#}-\xi_i-\xi_j)$ when $i \neq j$. Thus we do generate a *NTP* S-ring; clearly many of these are equivalent.

For the remainder of this section we consider irrationality. Consider first $n = 9$. There are only two rational primitive S-rings, one trivial, in this case, which implies we need only consider an orbit pattern of 4-4 with a trivial rational closure. But then $\overline{H^\#} = \theta + \theta^*$ and $\theta^2 = \theta^* + 2\nu$ with $|\nu| = 6$, an impossibility since $4 \nmid 6$.

For the remaining two cases consider first a note of importance. Let us assume $\eta = \sum_{i=1}^{t} \theta_i$. Because $|\theta_1| = \ldots = |\theta_t|$, and because η is in fact some $\xi_i = \sum_{j=1}^{u_i} \zeta_{i_j}$, we can easily check that any θ_i must have the same number of points in common with each ζ_{i_j}; thus we can conclude $t = 1,2$ or 4 when $n = 25$, and $t = 1,2,3$ or 6 when $n = 49$. When $n = 49$ and $t = 3$, or $n = 25$ and $t = 2$ we see that for each $x \in \theta_i$, $x^{-1} \in \theta_i$ and so $\theta_i^2 = \theta_i^{(2)} + |\theta_i| \cdot e + 2\nu$. When $n = 49$ and $t = 2$, $\theta_i \ni x$, x^2 and x^4, so that $\theta_i^2 = \theta_i + 2\theta_i^* + 2\nu$ for some $\nu \neq e$. We write $x + x^2 + x^4$ as $x^{[2]}$.

Consider $n = 25$, in which case the possible rational closures have orbit patterns 8-8-8, 8-16, 12-12 and 0-24 (indicating the trivial case $\eta_1 = \overline{H^\#}$). When $|\eta| = 8$, t cannot be 4, so we need only consider (WLOG) $\theta_1 = a + a^4 + b + b^4$. Then $\theta_1^2 = \theta_1^{(2)} + 4e + 2(ab + a^4b^4 + ab^4 + a^4b)$, and it can be verified that with $\theta_{11} = \theta_1$ and $\theta_{21} = ab + a^4b^4 + ab^4 + a^4b$ we have a basis for a *NTP* S-ring of orbit pattern 4-4-4-4-8. Note it can

also be shown that the orbit pattern 4-4-4-4-4-4 is inadmissible. A rational element of length 16 can appear either as $\eta_2 = \theta_{21} + \theta_{21}^{(2)}$ or as $\eta_2 = \sum_{i=1}^{4} \theta_{21}^{(i)}$. As considered for $n = 9$, $t \neq 4$, and computer analysis reveals the $t = 2$ choice as an invalid possibility. With $|\eta| = 12$ and $t = 4$ we have (WLOG) $\theta_1 = a + b + x$ with $x \notin \{a, b, e\}$. It is easily checked that the only x for which the ring condition holds is a^4b^4, in which case it can be verified that with $\theta_{11} = \theta_1$ and $\theta_{21} = ab^2 + a^3b^4 + ab^4$ we generate a *NTP* *S*-ring of orbit pattern 3-3-3-3-3-3-3-3. Now we examine $t = 2$, for which WLOG $\theta_1 = a + a^4 + b + b^4 + x + x^4$ so that $\theta_1^2 = \theta_1^{(2)} + 6e + 2\nu$ with $|\nu| = 12$. It is not difficult to check (with the computer) that with $x = ab$, $\theta_{11} = \theta_1$ and $\theta_{21} = ab^2 + a^4b^3 + a^2b + a^3b^4 + ab^4 + a^4b$ we have a valid basis for a *NTP* *S*-ring. Finally we have that for a rational element of length 24, $t \neq 4$ since $6 \nmid (36-6)/2$, and $t \neq 2$ since computer analysis reveals that in all possible choices for θ_1, θ_1^2 contains elements with at least 3 different coefficients.

With regard to the irrational case for $n = 49$, the most reasonable approach is to present only a summary of the results, for the work necessary to produce these results is tedious and involves considerable analysis, which is similar to that used with $n = 25$, of computer output. In order to give an idea of what is involved, consider the following. First, rational closures may have orbit patterns 12-12-12-12, 12-12-24, 12-18-18, 12-36, 18-30, 24-24 and 0-48. Clearly some cases are easily ruled inadmissible. For instance $|\eta| \neq 48$ with $t = 2$ since this implies $\theta_1^2 = \theta_1 + 2\theta_1^{(3)} + 2\nu$, whereas $24 \nmid (24^2 - 3 \cdot 24)/2$.

First the machine was used to obtain those θ_{ij} satisfying the ring condition for θ_{ij}^2. Secondly, each of these θ_{ij} must be considered

in its relation to other θ_{kl}. For instance, with $|\eta_1| = 12$ and $t = 2$ we see that $\theta_{11}^2 = (a^{[2]} + b^{[2]})^2 = \theta_{11} + 2\theta_{11}^{(3)} + 2[(ab)^{[2]} + (ab^2)^{[2]} + (ab^4)^{[2]}]$, and hence θ_{11} is acceptable in the first respect. However, it can be shown that the final term satisfies two different possibilities, for it is both an element of length 9 formed when $|\eta| = 18$ and $t = 2$, and the sum of 3 elements of length 3 formed when $|\eta| = 18$ and $t = 6$. Many similar cases exist. Finally, in all cases we must verify that $\theta_{ij} \cdot \theta_{kl}$ satisfies the ring condition; here the computer was used again.

The five resulting irrational S-rings are listed in the appendix, and thus we conclude the case $n = p^2$. We should remark that the cases with $p > 7$ are likely to be considerably more involved, probably even out of the range of machine computation, and hence are likely to require more refined techniques in the irrational cases.

§3.5 The case $n = p^m$, $m > 2$

Since Scott (10) has shown that groups of order 8 and 32 are B-groups, we really only need to consider $n = 16$ or 27. However, we shall, as indicated in §3.1, demonstrate that a group of order 32 is a B-group.

We shall first quite briefly consider $n = 16$, for which we must consider 3 Abelian groups H, namely, $\langle a \rangle \times \langle b \rangle \times \langle c \rangle \times \langle d \rangle$ with $a^2 = b^2 = c^2 = d^2 = 1$, $\langle a \rangle \times \langle b \rangle \times \langle c \rangle$ with $a^4 = b^2 = c^2 = 1$, and $\langle a \rangle \times \langle b \rangle$ with $a^4 = b^4 = 1$. By a sufficiently detailed consideration which contains no notions of importance, the results which follow can be derived. However, the results are merely quoted since the analysis is moderately lengthy, and since they have also been obtained using the computer.

It is easily seen that, in the rational case, only the orbit patterns 5-5-5, 5-10 and 6-9 must be considered. We note that given an η_1 satisfying the ring property, we can generate one S-ring with $\overline{H^{\#}}-\eta_1$; however, we must also consider a possible orbit pattern of 5-5-5 when $|\eta_1| = 5$. We now list the acceptable quantities η_1 for each of the 3 groups:

1. (a) $a+b+c+d+abcd$; (b) $a+b+c+d+ab+cd$;

2. (a) $a+a^3+b+c+a^2bc$; (b) $a+a^3+a^2+b+c+a^2bc$;

3. (a) $a+a^3+b+b^3+a^2b^2$; (b) $a+a^3+b+b^3+a^2+b^2$;
(c) $a+a^3+b+b^3+ab+a^3b^3$.

In each case the choice (a) has length 5, so we must consider the orbit pattern 5-5-5. But, in case 1, we know that one of the elements of η is the product of the other 4. Thus, it is easily checked that we obtain only one further NTP S-ring: $\eta_2 = abc+abd+ab+ad+bc$, $\eta_3 = bcd+acd+cd+ac+bd$. In case 2, an η of length 5 must contain 3 elements of order 2, whereas H contains only 7, so we can omit the orbit pattern 5-5-5. Similarly, in case 3, we obtain one further NTP S-ring with $\eta_2 = ab+a^3b^3+a^2b+a^2b^3+a^2$ and $\eta_3 = ab^3+a^3b+ab^2+a^3b^2+b^2$, to give a total of 9 rational NTP S-rings, three of which are of course Wielandt S-rings.

Now there remains only the irrational case. Certainly 3-3-9 and 5-5-5 are the only orbit patterns allowable, as each element has 1 or 2 conjugates. Trivially all elements are rational in the first group; in the second two, irrational elements must contain no elements of order 2, leaving only the case in which the rational closure has $\eta_1 = a+a^3+b+b^3+ab+a^3b^3$. Then if $\eta = \theta+\theta^*$, $\theta^2 = \theta^*+2\nu$ with $|\nu| = 3$,

a possibility only when $\theta = a + b + a^3b^3$. But then $\theta\theta^* = 3e + a + a^3 + b + b^3 + ab^3 + a^3b$, a contradiction to the ring property. Thus we have concluded the case $n = 16$.

When $n = 27$ we have by §2.3 that *NTP* S-rings may be admitted only over $H = \langle a\rangle \times \langle b\rangle \times \langle c\rangle$ with $a^3 = b^3 = c^3 = 1$. Since each element has a trace of length 2, all rational orbits have even length; it is easily checked that $6 \leq r_1 \leq 12$. Noting that $\eta^{(2)} = \eta$, we have $\eta^2 = r\cdot e + \eta + 2\nu$ where $|\nu| = (r^2-2r)/2$. With $r_1 = 12$, $|\nu| = 60 \neq x\cdot 12 + y\cdot 14$ for any non-negative integers x and y with $y \neq 0$, whereas the only orbit pattern with $r_1 = 12$ is 12–14. With $r_1 = 10$, $|\nu| = 40$, which is similarly not equal to $x\cdot 10 + y\cdot 16$. When $r_1 = 8$ we may have orbit patterns 8–8–10 or 8–18. Now $|\nu| = 24$ so we need not consider 8–18, but we could have in the 8–8–10 case that $\eta_1(N_2) \neq 0$. However (WLOG) $\eta_1 = tr(a + b + c + x)$ with $x \in H - \{a,b,c,1\}$ so that $\eta_1^2(h) \neq 0$ for more than 8 elements h which are not in η_1. Thus we consider $r_1 = 6$, in which case (WLOG) $\eta_1 = tr(a + b + c)$ and $\eta_1^2 = r\cdot e + \eta_1 + 2tr(ab + ab^2 + ac + ac^2 + bc + bc^2)$. Clearly, choosing $\eta_2 = \eta_1^2 - r\cdot e - \eta_1$ and $\eta_3 = \overline{H^{\#}} - \eta_1 - \eta_2$ generates the Wielandt S-ring, but we still must consider the pattern 6–6–6–8. However, if w is a rational basis element of length 6 (which must, by consideration of η_1^2, be formed from the elements of η_2), we have $w^2 = 6e + w + 2\nu_0$ with $|\nu_0| = 12$. But w^2 contains an element of η_3, an impossible situation.

And so we consider the admissibility of irrational S-rings. Because each element has exactly 2 conjugates, and $|\eta^*| = |\eta|$, all irrational orbits θ have a length of 3, 4, 6 or 13; further, we know its rational closure has an orbit pattern 6–8–12 or 0–26. Now $|\theta| = 3$ implies WLOG that $\theta = a + b + c$; thus $ab + ac + bc$ must be a basis element, which is not possible. Considering $|\theta| = 4$ requires $\theta^2 = \theta^* + 2\nu$ with

$|\nu| = 6$, so that $\nu = \eta_1$ whereas θ^2 contains elements of η_2. Next, the fact that there are no non-negative integers x, y for which $15 = x \cdot 6 + y \cdot 8$ contradicts the existence of an irrational basis element of length 6, leaving only the 13-13 case. Computer analysis of the 2^{10} cases (assuming WLOG that $a,b,c \in \theta$) admits 36 valid expressions for θ; further computer analysis reveals all are equivalent. Thus with $\theta = a + b + c + ab + ab^2 + bc + bc^2 + ca + ca^2 + abc + a^2b^2c + a^2bc^2 + ab^2c^2$ we obtain one *NTP S*-ring in addition to the Wielandt one.

We now wish to show that no *NTP S*-rings are permitted when $n = 32$. There are three Abelian groups H for which *NTP S*-rings are not disallowed by the theorems of Chapter II, namely, $\langle a\rangle \times \langle b\rangle \times \langle c\rangle \times \langle d\rangle \times \langle f\rangle$ with $a^2 = \dots = f^2 = 1$, $\langle a\rangle \times \langle b\rangle \times \langle c\rangle \times \langle d\rangle$ with $a^4 = b^2 = c^2 = d^2 = 1$, and $\langle a\rangle \times \langle b\rangle \times \langle c\rangle$ with $a^4 = b^4 = c^2 = 1$.

Assuming rationality we must have $r \geqslant 5$ in order that $\langle N\rangle$ be H. We can eliminate the orbit patterns 5-6-20 and 9-10-12, for these violate Theorem 1.7.2. In 5-5-5-6-10, $\eta_1\eta_4 = \eta_2\eta_4 = \eta_3\eta_4 = 3\eta_5$ (by 1.7.2). Consequently $\eta_4\overline{H} = 9\eta_5 + \dots$, whereas $\eta_4\overline{H} = 6\overline{H}$. Similarly 5-8-8-10 is eliminated. Now, for any η, we may write $\eta^2 = \eta^{(2)} + 2w$ for some w. Secondly, if $x \in N \cap K_2$, $x^2 = e$; if $x \in N \cap K_4$ then $x^2 = (x^*)^2$. As a result we may write $\eta^2 = |\eta| \cdot e + 2\nu$ for some $\nu \not\ni e$.

We now wish to examine the case 6-10-15, and here we will in fact discover 3 non-trivial *S*-rings. However, by examining the largest basis element, rather than the smallest as usual, we will find these to be imprimitive.

First we find by a simple length argument that $\eta_1\eta_2$ must be one of the following: $4\eta_3$, $2\eta_3 + 3\eta_2$, $2\eta_3 + 5\eta_1$, $10\eta_1$, $6\eta_2$ or $3\eta_2 + 5\eta_1$.

Similarly we have $\eta_1^2 = 6e + 2\eta_3$. Applying 1.7.1 with $\eta_3 = \eta_1$ (in the theorem) we see that the coefficient of η_1 in $\eta_1\eta_2$ must be 0, leaving three choices for $\eta_1\eta_2$.

Now we introduce any subgroup K of index 2 in H, and indicate $|K \cap N_1|$ by k. Since $\eta_1^2 = 6e + 2\eta_3$ we have $|K \cap N_3| = k^2-6k+15$; thus $|K \cap N_2| = 16 - [1 + k + (k^2-6k+15)] = 5k - k^2$. Since we now know how η_1 and η_2 occur with regard to K, we see that $\eta_1\eta_2$ contains $k(5k-k^2) + (6-k)(10+k^2-5k)$ elements of K. We have noted previously that we must consider 3 groups of order 32; look now at the first. Because $\langle N_1 \rangle = H$, η_1 (WLOG) is given by $\eta_1 = a+b+c+d+f+x$. Further, by examination of those K of index 2 generated by a subset of a, b, c, d and f, we see it follows that (with a similar argument applied to the other two groups) that $k = 4$ or 5 for some such subgroup K.

Let us now assume $\eta_1\eta_2 = 3\eta_2 + 2\eta_3$. Using the right hand expression we can recompute the number of elements of K in $\eta_1\eta_2$. If in fact we do have an S-ring, these two values must be equal. By computation it follows that this is not true in this case; equality occurs only when $\eta_1\eta_2 = 4\eta_3$ and $k = 4$. We may WLOG assume that η_1 has one of the following forms (where it is clear to which of the three groups we refer in each case), where $x_i \in K_2$:

(1) $a+b+c+d+f+x_1$,

(2) $a+a^3+b+c+d+x_2$, (3) $a+a^3+ab+a^3b+c+d$,

(4) $a+a^3+b+b^3+c+x_3$, (5) $a+a^3+b+b^3+ac+a^3c$.

In cases 3 and 5, $\eta_1(a^2) = 4$, a contradiction to $\eta_1^2 = 6e + 2\eta_3$. In the remaining cases, $k = 5$ for some subgroup K except when $x_1 = abcdf$, $x_2 = a^2bcd$ or bcd and $x_3 = a^2c$, b^2c or a^2b^2c. With $x_2 = bcd$ or $x_3 = a^2c$ or

b^2c, there is some y in η_1^2 with coefficient 4; hence we eliminate these cases. In each remaining case, $\eta_3^2 = 15e + 14\eta_3$, a contradiction to primitivity. However, computation verifies that in each of these three last cases we obtain an imprimitive S-ring.

The approach to 7-10-15 is similar but the work simpler. By 1.7.2, $\eta_1\eta_2 = 5\eta_3$. Secondly $\eta_1^2 = 7e + 2\eta_1 + 2\eta_3$ by a length argument. Consequently we again obtain two polynomials in k for the number of elements of K in $\eta_1\eta_2$. However these are equal for none of the possible values of k, so we conclude no basis is admitted with this orbit pattern.

Finally, we have only to consider 5-5-6-15 and 5-6-10-10. We first note (WLOG) the three cases for η_1: $a+b+c+d+f$, $a+a^3+b+c+d$ and $a+a^3+b+b^3+c$. By squaring η_1 in each case we find that ν contains 10 elements with coefficient 1. Consequently, in the first case (because $|\nu| = 10$) $\eta_1^2 = 5e + 2\eta_1 + 2\eta_2$, although in all of the cases $\eta_1(N_1) = 0$. In the final case WLOG $\eta_1^2 = 5e + 2\eta_3$. However, for each of the definitions of η_1, the resulting η_3 may be squared, and will be found to be invalid

Consequently there are no rational S-rings. Since H always contains an element of order 2, which is by definition its own conjugate, there are no irrational S-rings, and we can now conclude H is a B-group.

§3.6 The case $n = 36$

Applying the results of Chapter II to this case, we see that all S-rings must occur over $H = \langle a\rangle \times \langle b\rangle \times \langle c\rangle \times \langle d\rangle$ where $a^2 = b^2 = c^3 = d^3 = e$. Since we can write $H = \langle ac\rangle \times \langle bd\rangle$, we know by §2.2 that H admits a *NTP* Wielandt S-ring. We wish to show there are exactly 2 others.

First we have, for any $x \in K_3$ and $y \in K_{2,1}$, that $\eta^{(2)} \ni x, x^2$ when $\eta \ni yx$. Secondly, δ_2 requires there be a $y' \in K_{2,1}$ $(\neq y)$ such that $y'x \ni \eta$. As well, since $\langle\eta\rangle$ must be H, η is required to contain 2 elements

x_1, x_2 of $K_{3,6}$ with $x_2 \notin \langle x_1 \rangle$. Thus $4|(r-5)$ and $r \geq 8$. For $s_1 = 0$ we only need consider $r_1 = 8$; to satisfy δ_2, $\eta_1 = tr(ac+bd+xc+yd)$ with $x,y \in K_{2,1}$. However, this violates δ_3 regardless of the choice of x and y.

Since Scott's procedure allows no orbit pattern with $s_1 = 1$, we now consider $s_1 = 2$. If $r_1 = 10$, then by δ_2, η_1 must be (WLOG) $tr(a+b+x_1c+x_2c+y_1d+y_2d)$ with $x_1, x_2, y_1, y_2 \in K_{2,1}$. Now $\eta^{(3)} = a+b+2(x_1+x_2+y_1+y_2)$, and noting that $x_1 \neq x_2$ and $y_1 \neq y_2$, δ_3 requires that $x_1 = a$, $y_1 = b$ and $x_2 = y_2 = 1$. This, with $\eta_2 = \overline{H^{\#}} - \eta_1$, yields the Wielandt S-ring. The fact that H contains only one further element of order 2 disallows the possibility of an orbit pattern 10-10-15. If $r_1 = 14$, $\eta_1 = tr(a+b+x_1c+x_2c+y_1d+y_2d+z_1c_1+z_2c_2)$ with $x_1, x_2, y_1, y_2, z_1, z_2 \in K_{2,1}$ and $c_1 \in K_3$. But $\eta^{(3)} \equiv \delta_3 \cdot 1 \pmod 3$ and $\eta^{(3)} = a+b+2\sum_{i=1}^{2}(x_i+y_i+z_i)$ can be simultaneously satisfied only when either one or four of the x_i, y_i and z_i are a. However, the appearance of a four times would contradict the fact that $x_1 \neq x_2$, $y_1 \neq y_2$ and $z_1 \neq z_2$. Thus (WLOG) x_1, and only x_1, is a. Similarly exactly one of the others, not x_2, is b. Thus four remain undetermined and, as noted above, not all are equal, so that one of them must be 1 and three ab. Again the inequalities $y_1 \neq y_2$ and $z_1 \neq z_2$ show that $\eta_1 = tr(a+b+ac+abc+bd+abd+c_1+abc_1)$, which with $\overline{H^{\#}} - \eta_1$, yields a basis for a *NTP* S-ring. By consideration of the group isomorphism $d \to d^2$, with a,b and c fixed, we see that there is only one unique S-ring.

Finally, for $s_1 = 3$, $r_1 = 15$. WLOG $\eta_1 = tr(a+b+ab+x_1c+x_2c+y_1d+y_2d+z_1c_1+z_2c_2)$ with $x_1, x_2, y_1, y_2, z_1, z_2 \in K_{2,1}$ and $c_1 \in K_3$. It is easily verified (as above)

that δ_3 is satisfied only when $\eta_1 = tr(a+b+ab+ac+c+bd+d+abc_1+c_1)$, again yielding a *NTP* S-ring with $\overline{H^{\#}}-\eta_1$. As we did for $r_1 = 14$, assume WLOG that $c_1 = cd$; consequently we conclude there are 3 rational *NTP* S-rings when $n = 36$.

By Theorem 1.6.3 only the last of these can be considered as a possible rational closure for an irrational *NTP* S-ring. However the computer was used to show that none of the 2^{10} cases satisfies the ring condition, so we conclude that the only *NTP* S-rings are those mentioned.

CHAPTER IV

THE CASE $H = 72$

§4.1 Introduction

We will now consider a group for which no *NTP* *S*-rings are known, and show in fact, that none exist. This group has special significance in that it is, as mentioned in Chapter II, the smallest of a class not covered by Bercov's result (2.3.3); consequently, the result obtained in this chapter indicates that Bercov's result may be valid in a more general form.

The theorems of Chapter II eliminate from consideration all but two cases, namely, $H = \langle a\rangle \times \langle b\rangle \times \langle c\rangle \times \langle d\rangle \times \langle f\rangle$ with $a^2 = b^2 = c^2 = d^3 = f^3 = e$ and $H = \langle a\rangle \times \langle b\rangle \times \langle c\rangle \times \langle d\rangle$ with $a^4 = b^2 = c^3 = d^3 = e$. Because the analysis resembles §3.6 more closely, we first consider the former case. In both cases, the notation and ideas of Chapter III are used.

§4.2 The 2-2-2-3-3 case

First, δ_3 implies $r \geqslant 9$. Furthermore, 9 elements satisfying δ_2 violate δ_3; thus $r \geqslant 10$. Now $r = 10$ requires WLOG that $\eta = tr(ad + d + bf + f + a + b)$, in which case $\langle N\rangle < H$; thus $r \geqslant 11$. We now demonstrate that $r_1 = 13$, 16 and 21 are not acceptable cases, and note that this will remain true in §4.3. For, with $r_1 = 13$ the only permissible orbit patterns are 13-14-18-26 and 13-16-16-26. The first implies $\eta_1\eta_2 = 7\eta_4$ and $\eta_1\eta_3 = 9\eta_4$ (by 1.7.2), so that $\eta_1\overline{H} = \eta_1\sum_{i=0}^{4}\eta_i = \eta_1 + \eta_1\eta_4 + \eta_1^2 + 16\eta_4$. But $\eta_1\overline{H} = 13\overline{H}$, a contradiction. The second case with $r_1 = 13$ is disallowed identically, and $r_1 = 16$ or 21

simply violates 1.7.2, so that only the cases $r_1 = 11$, 12, 14, 15, 17 and 20 remain to be considered.

When $r_1 = 11$, s_1 must be 3, so WLOG $\eta_1 = tr(a+b+c+ad+bd+cf+f)$. Thus $\eta_1(f) = 4 \neq \eta_1(a)$, a contradiction. To have $r_1 = 12$ requires $s_1 = 0$ or 4. The former case has $\eta_1 = tr(xd+yd+xf+yf+xd_1+yd_1)$ with $x,y \in K_{2,1}$ and $d_1 \in K_3$, a contradiction since $<N_1> < H$. In the latter case $\eta_1 = tr(a+b+c+x+ad+bd+cf+xf)$ with $x \in K_2$. At this point we introduce a notational liberty to be used in this chapter by writing $\eta_1(\{ac,bc,ax,bx\}) = 2$ and $\eta_1(\{ab,cx\}) = 6$ in order to say that ac, bc, ax and bx appear twice in η_1^2, and ab and cx appear 6 times. From this it is immediate that $x \neq ab$, ac or bc. Further, with $x = abc$, $\eta_1(ab) = 12$, another impossibility. Thus we may consider $r_1 = 14$; $s_1 = 2$ or 6. First, δ_3 makes the latter impossible; we consequently examine $\eta_1 = tr(a+b+ad+cd+bf+cf+d_1+cd_1)$ with $d_1 \in K_3$. In this case $\eta_1(a) = 0 \neq \eta_1(d_1)$, so we conclude $r_1 \geq 15$. Next we have $r_1 = 15$ with $s_1 = 3$ or 7, the latter violating δ_3 and the former occuring (WLOG) as $\eta_1 = tr(a+b+c+ad+xd+bf+xf+cdf+xdf)$ with $x \in K_{2,1}$. Since $\eta_1(\{ab,bc,ac\}) = 2$ and $\eta_1(\{ax,bx,cx\}) = 4$, we must have $x = abc$ or 1 in order that $\eta_1(a) = \eta_1(b) = \eta_1(c)$. But when $x = 1$ we have $\eta_1(d) = 6 \neq \eta_1(a)$. When $x = abc$, we conclude by considering the possible orbit patterns, that $tr\left(ab+bc+ac+(d+f+df+df^2)(1+ab+ac+bc)\right)$ must be a basis element η_2, for all these elements occur in η_1^2 with equal coefficient. However $\eta_3(ab) = 34$, which implies $\eta_3^2 = 35e+34\eta_3$, and thus that $<N_3> < H$, a contradiction.

Now only two cases remain. Since one has orbit pattern 17-20-34 and the other 20-21-30 it is sufficient to show that a basis element of length 20 is inadmissable. Now $r = 20$ yields $s = 0$ or 4; when $s = 4$ three

cases are admitted: $\eta = tr(a+b+c+x+ad+yd+bf+yf+cdf+ydf+xdf^2+df^2)$, $\eta = tr(a+b+c+x+ad+bd+cf+yf+xdf+ydf+df^2+ydf^2)$ and $\eta = tr(a+b+c+x+ad+bd+cd+yd+xf+yf+yf_1+f_1)$ where $x \in K_2$, $y \in K_{2,1}$ and $f_1 \in K_3$. However, in each case it can be verified that η_1^2 does not satisfy the ring condition. For $s = 0$, only $\eta = tr(ad+cd+bd+d+af+bf+adf+cdf+bdf^2+cdf^2)$ is admissible. However $\eta(d) \neq \eta(f)$, so that we can now conclude that this group of order 72 admits no rational primitive S-rings except the trivial one.

In fact we can say it has none at all. For, given any irrational basis element, we know its trace must be $\overline{H^{\#}}$. As well, some basis element contains an element of order 2, and consequently intersects all of its conjugates. Clearly then, any irrational basis is trivial.

§4.3 The 4-2-3-3 case

We now wish to consider the second group of order 72, and we first note that $\langle N \rangle = H$ and δ_2 imply $r \geqslant 8$. Much simplification results by considering the following properties that the elements of η must satisfy. Since $x \in K_4$ implies $(tr\, x)^{(3)} = tr\, x$, $c_0 \in K_3$ implies $(tr\, xc_0)^{(3)} = 2\, tr\, x$, and elements of order 2, 3 or 6 cannot have a cube of order 4, we must have, in order to satisfy δ_3, for $r \leqslant 20$, that $|N \cap K_{12}| = 8$ when $|N \cap K_4| = 4$. Similarly, with $|N \cap K_4| = 0$, $|N \cap K_{12}| = 12$ and with $|N \cap K_4| = 2$, $|N \cap K_{12}| = 4$ or 16. By application of δ_3, we see that $|N \cap K_{3,6}| = 0$ is possible only when $s = 0$, that $|N \cap K_{3,6}| = 4$ is impossible with $s = 0$ or 3, and that $|N \cap K_{3,6}| = 8$ permits only $s = 2$ or 3.

Having dismissed $r_1 = 13$, 16 and 21 in §4.2, we consider the remaining cases, again noting that both $r_1 = 17$ and $r_1 = 20$ are eliminated by showing r cannot be 20. Writing *type* s-u_2-u_3-u_4 to indicate η contains u_2 elements of order 3 or 6, u_3 of 4 and u_4 of 12, we can easily verify that the only types satisfying the conditions outlined in the previous paragraph are 1-4-2-4, 0-0-0-12, 2-4-2-4, 0-0-4-8, 1-4-0-12, 3-8-2-4, 1-4-4-8 and 2-12-2-4. The fifth, sixth and seventh belong to the case with $r_1 = 17$ and so need not be considered.

In the discussion of these cases, we assume $x,y,z \in K_2$ and $v \in K_4$. With type 1-4-2-4, (WLOG) $\eta_1 = tr(x + xc + c + v + vd)$, so that $\eta_1(c) = 4$ and $\eta_1(\nu) \neq 4$, a contradiction. For 0-0-0-12, $\eta_1 = tr(vc + vd + vd_1)$ with $d_1 \in K_3$, in which case $\langle N\rangle < H$. In 2-4-2-4, $\eta_1 = tr(x + y + xc + yc + v + vd)$, implying $\eta_1(v^2) = \eta_1(xy) = 6$ and $\eta_1(x) = \eta_1(y) = 0$. Since $v^2 = x$ (or y) makes $\eta_1(x) \neq \eta_1(y)$, we conclude $v^2 = xy$, so that $\eta_1(xy) = 12$ and $|\eta_1^2| > 144$. Thus we must consider 0-0-4-8 which we eliminate by virtue of $\eta_1(a^2)$ being 12 when $\eta_1 = tr(a + ab + ac + abd)$. Finally, when we consider type 2-12-2-4, $\eta = tr(x + y + xc + zc + yd + zd + d_1 + zd_1 + v + vc_1)$ with $c_1, d_1 \in K_3$. Since $v^2 = a^2$ we have $\eta(x) = \eta(y) = 4$ and $\eta(z) = \eta(a^2) = 6$. Because $\eta(x)$ must equal $\eta(y)$, $v^2 \neq x$ (or y) and $\eta(a^2) = 12$. Consequently, in the case 17-20-34 we have $\eta_2(N_2) = 4$ and $\eta_2(N_i) = 12$ with $i = 1$ or 3. This contradicts $|\eta_2^2| = \sum_{j=0}^{3} c_j|\eta_j|$. Eliminating 20-21-30 similarly, we conclude the group admits no rational *NTP* S-rings.

Irrational S-rings being eliminated as in §4.2, we can now conclude that any group of order 72 is a B-group.

BIBLIOGRAPHY

1. W. Burnside, 1906, On simply transitive groups of prime degree, Quart. J. Math., 37, 215-221.

2. __________, 1911, Theory of Groups of Finite Order, 2nd ed., Cambridge Univ. Press.

3. R.D. Bercov, 1965, The double transitivity of a class of permutation groups, Can. J. Math., 17, 480-493.

4. R. Kochendörffer, 1937, Untersuchungen über eine Vermutung von W. Burnside, Schr. Math. Sem. Inst. angew. Math. Univ. Berlin, 3, 155-180.

5. D. Manning, 1936, On simply transitive groups with transitive Abelian subgroups of the same degree, Trans. A.M.S., 40, 324-342.

6. O. Nagai, 1961, On transitive groups that contain non-Abelian regular subgroups, Osaka Math. J., 13, 199-207.

7. H. Nagao, 1963, On transitive groups of degree 3p, J. Math., Osaka City Univ., 14, 23-33.

8. I. Schur, 1933, Zur Theorie der einfach transitiven Permutationsgruppen, Sitzungsberichte Preuss Akad. Wiss., phys.-math. Kl., 598-623.

9. W.R. Scott, 1957, Solvable factorizable groups, Illinois J. Math., 1, 389-394.

10. __________, 1964, Group Theory, Prentice-Hall, Englewood Cliffs, N.J.

11. H. Wielandt, 1935, Zur Theorie der einfach transitiven Permutationsgruppen, Math. Z., 40, 582-587.

12. __________ , 1949, Zur Theorie der einfach transitiven Permutationsgruppen, II, Math. Z., 52, 384-393.

13. __________ , 1962, Permutation Groups, Lectures at the Univ. of Tübingen, 1954-55, prepared by J. André, translated from the German by R. Bercov (Cal. Tech., 1962).

APPENDIX

S-RINGS OVER ABELIAN GROUPS H, $|H| \leqslant 50$

The following table lists all S-rings occurring over Abelian groups whose order is $\leqslant 50$. In the table, certain conventions will be followed for reasons mostly of convenience, both in construction and interpretation.

For each $n(=|H|)$, the section of Chapter III where the structure of the group (e.g. $H = \langle a \rangle$) is defined is given; that structure is used to write the bases for the S-rings given. When more than one group structure is defined in the section, it is clear from the basis itself which structure is applicable. In the rational cases, when $\eta_2 = \overline{H^{\#}} - \eta_1$, η_2 will not be listed. In the irrational cases, only one of a group of conjugates will be listed. In fact, when $n = p$, only the first two elements of a basis element will be listed, for if $a, a^x \in \theta$, then clearly $\theta = a + a^x + a^{x^2} + \ldots + a^{x^{d-1}}$ where $a^{x^d} = a$. Further, when $n = p$, the case $\theta_{11} = a + a^{p-1}$ will not be listed since it occurs for all p. Rationality is indicated by η; irrationality by θ.

n	section	basis
7	3	1. $\theta = a + a^2$
9	4	1. $\eta_1 = a + a^2 + b + b^2$
11	3	1. $\theta = a + a^3$
13	3	1. $\theta = a + a^3$
		2. $\theta = a + a^5$
		3. $\theta = a + a^4$

n	section	basis
16	5	1. $\eta_1 = a+b+c+d+abcd$
		(a) $\eta_2 = \overline{H^{\#}} - \eta_1$
		(b) $\eta_2 = abc+abd+d+ad+bc$
		$\eta_3 = bcd+acd+cd+ac+bd$
		2. $\eta_1 = a+b+c+d+ab+cd$
		3. $\eta_1 = a+a^3+b+c+a^2bc$
		4. $\eta_1 = a+a^3+a^2+b+c+a^2bc$
		5. $\eta_1 = a+a^3+b+b^3+a^2b^2$
		(a) $\eta_2 = \overline{H^{\#}} - \eta_1$
		(b) $\eta_2 = ab+a^3b^3+a^2b+a^2b^3+a^2$
		$\eta_3 = ab^3+a^3b+ab^2+a^3b^2+b^2$
		6. $\eta_1 = a+a^3+b+b^3+a^2+b^2$
		7. $\eta_1 = a+a^3+b+b^3+ab+a^3b^3$
17	3	1. $\theta = a+a^4$
		2. $\theta = a+a^2$
19	3	1. $\theta = a+a^7$
		2. $\theta = a+a^4$
		3. $\theta = a+a^8$
23	3	1. $\theta = a+a^2$
25	4	1. $\theta_{11} = a+a^4+b+b^4$
		$\theta_{21} = ab+a^4b^4+ab^4+a^4b$
		$\eta_3 = tr(ab^2+ab^3)$
		2. $\theta_{11} = a+b+a^4b^4$
		$\theta_{21} = ab^2+a^3b^4+ab^4$
		3. $\theta_{11} = a+a^4+b+b^4+x+x^4$
		$\theta_{21} = ab^2+a^4b^3+a^2b+a^3b^4+ab^4+a^4b$

n	section	basis
25	4	4. $\eta_1 = tr(a + b)$
		5. $\eta_1 = tr(a + b + ab)$
		6. $\eta_1 = tr(a + b)$
		$\eta_2 = tr(ab + ab^2)$
		$\eta_3 = tr(ab^3 + ab^4)$
		7. $\eta_1 = tr(a + b)$
		$\eta_2 = tr(ab + ab^4)$
		$\eta_3 = tr(ab^2 + ab^3)$
27	5	1. $\eta_1 = a + a^2 + b + b^2 + c + c^2$
		$\eta_2 = tr(ab + ab^2 + ac + ac^2 + bc + bc^2)$
		$\eta_3 = tr(abc + abc^2 + ab^2c + ab^2c)$
		2. $\theta = a + b + c + ab + ab^2 + bc + bc^2 + ca + ca^2 + a^2b^2c + a^2bc^2 + ab^2c^2$
29	3	1. $\theta = a + a^{12}$
		2. $\theta = a + a^7$
		3. $\theta = a + a^4$
31	3	1. $\theta = a + a^5$
		2. $\theta = a + a^2$
		3. $\theta = a + a^6$
		4. $\theta = a + a^{15}$
		5. $\theta = a + a^7$
36	6	1. $\eta_1 = tr(a + b + ac + c + bd + d)$
		2. $\eta_1 = tr(a + b + ac + abc + bd + abd + cd + abcd)$
		3. $\eta_1 = tr(a + b + ab + ac + c + bd + d + abcd + cd)$

n	section	basis		
37	3	1.	θ	$= a + a^{10}$
		2.	θ	$= a + a^{6}$
		3.	θ	$= a + a^{11}$
		4.	θ	$= a + a^{7}$
		5.	θ	$= a + a^{8}$
		6.	θ	$= a + a^{3}$
41	3	1.	θ	$= a + a^{9}$
		2.	θ	$= a + a^{10}$
		3.	θ	$= a + a^{3}$
		4.	θ	$= a + a^{4}$
		5.	θ	$= a + a^{2}$
43	3	1.	θ	$= a + a^{6}$
		2.	θ	$= a + a^{4}$
		3.	θ	$= a + a^{2}$
		4.	θ	$= a + a^{9}$
		5.	θ	$= a + a^{7}$
47	3	1.	θ	$= a + a^{2}$
49	4	1.	θ_{11}	$= a^{[2]} + b^{[2]}$
			θ_{11}	$= (ab)^{[2]} + (ab^{2})^{[2]} + (ab^{4})^{[2]}$
			η_{3}	$= tr(ab^{3} + ab^{5} + ab^{6})$
		2.	θ_{11}	$= a + a^{6} + b + b^{6} + ab + a^{6}b^{6} + a^{3}b^{6} + a^{4}b +$ $ab^{4} + a^{6}b^{3} + a^{3}b^{4} + a^{4}b^{3}$
			η_{2}	$= tr(ab^{3} + ab^{5})$

n	section	basis
49	4	3. $\theta_{11} = a + a^6 + b + b^6$
		$\theta_{21} = ab + a^6b^6 + ab^6 + a^6b$
		$\theta_{31} = a^2b + a^5b^6 + a^2b^6 + a^5b + ab^2 + a^6b^5 + a^3b^4 + a^4b^3$
		4. $\theta_{11} = a + a^6 + b + b^6 + ab + a^6b^6$
		$\theta_{21} = a^2b + a^5b^6 + ab^2 + a^6b^5 + ab^6 + a^6b$
		$\eta_3 = tr(ab^3 + ab^5)$
		$\theta_{11} = a + a^6 + b + b^6 + ab + a^6b^6 + ab^2 + a^6b^5 + ab^3 + a^6b^4 + a^2b + a^5b^6 + a^3b + a^4b^6 + a^2b^5 + a^5b^2$
		5. $\eta_1 = tr(a + b)$
		a) $\eta_2 = tr(ab + ab^2)$
		i) $\eta_3 = tr(ab^3 + ab^4)$
		$\eta_4 = tr(ab^5 + ab^6)$
		ii) $\eta_3 = tr(ab^3 + ab^5)$
		$\eta_4 = tr(ab^4 + ab^6)$
		iii) $\eta_3 = tr(ab^3 + ab^4 + ab^5 + ab^6)$
		b) $\eta_2 = tr(ab + ab^3)$
		i) $\eta_3 = tr(ab^2 + ab^5)$
		$\eta_4 = tr(ab^4 + ab^6)$
		ii) $\eta_3 = tr(ab^2 + ab^6)$
		$\eta_4 = tr(ab^4 + ab^5)$
		iii) $\eta_5 = tr(ab + ab^4 + ab^5 + ab^6)$
		c) $\eta_2 = tr(ab + ab^6)$
		$\eta_3 = tr(ab^2 + ab^3 + ab^4 + ab^5)$
		d) $\eta_2 = tr(ab + ab^2 + ab^3)$
		$\eta_3 = tr(ab^4 + ab^5 + ab^6)$

n	section	basis
49	4	5. e) $\eta_2 = tr(ab + ab^2 + ab^4)$
		$\eta_3 = tr(ab^3 + ab^5 + ab^6)$
		f) $\eta_2 = tr(ab + ab^2 + ab^5)$
		$\eta_3 = tr(ab^3 + ab^4 + ab^6)$
		g) $\eta_2 = \overline{H^{\#}} - \eta_1$
		6. $\eta_1 = tr(a + ab + ab)$
		7. $\eta_1 = tr(a + b + ab + ab^2)$
		8. $\eta_1 = tr(a + b + ab + ab^3)$

The following table gives the number of different rational and irrational non-trivial primitive S-rings occuring over Abelian groups of order n less than 50.

n	rational	irrational	n	rational	irrational
1	0	0	25	4	3
2	0	0	26	0	0
3	0	0	27	1	1
4	0	0	28	0	0
5	0	0	29	0	4
6	0	0	30	0	0
7	0	2	31	0	6
8	0	0	32	0	0
9	1	0	33	0	0
10	0	0	34	0	0
11	0	2	35	0	0
12	0	0	36	3	0
13	0	4	37	0	7
14	0	0	38	0	0
15	0	0	39	0	0
16	9	0	40	0	0
17	0	3	41	0	6
18	0	0	42	0	0
19	0	4	43	0	6
20	0	0	44	0	0
21	0	0	45	0	0
22	0	0	46	0	0
23	0	2	47	0	2
24	0	0	48	0	0
			49	14	4